

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-274928  
(43)Date of publication of application : 13.10.1998

(51)Int.Cl. G09C 1/00  
G06F 9/06  
H04L 9/32

(21)Application number : 09-342543 (71)Applicant : FUJI XEROX CO LTD  
(22)Date of filing : 12.12.1997 (72)Inventor : KAKEHI RUMIKO  
SAITO KAZUO

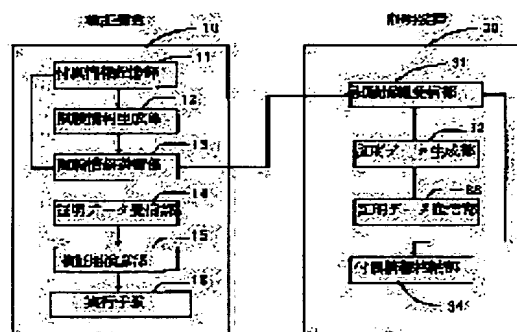
(30)Priority  
Priority number : 09 15079 Priority date : 29.01.1997 Priority country : JP

## (54) USER AUTHENTICATION DEVICE AND METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To safely transmit accessory information such as information intrinsic to digital intelligent property and the information recorded on a digital intelligent property side to a verification device in a user authentication procedure and to make a user able to confirm the accessory information transmitted in the process of the transmission.

**SOLUTION:** An accessory information storage part 11 stores the accessory information of a transmission object, a test information generation part 12 generates test information from the set of data for authentication and the accessory information and a test information transmission part 13 transmits the test information and the accessory information to the verification device 30. The test information reception part 31 of the verification device 30 receives the pair of the test information and the accessory information and a verification data generation part 32 generates verification data from the test information and the accessory information. In an accessory information storage part 34, the accessory information is recorded in an IC card. The verification data reception part 14 of the verification device 30 receives the verification data and an arithmetic part 15 for verification verifies the verification data.



Best Available Copy

## LEGAL STATUS

[Date of request for examination] 13.06.2002  
[Date of sending the examiner's decision of rejection]  
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]  
[Date of final disposal for application]  
[Patent number]  
[Date of registration]  
[Number of appeal against examiner's decision of rejection]  
[Date of requesting appeal against examiner's decision of rejection]  
[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-274928

(43) 公開日 平成10年(1998)10月13日

(51) Int.Cl.<sup>6</sup>

G 0 9 C 1/00

G 0 6 F 9/06

H 0 4 L 9/32

識別記号

6 4 0

5 5 0

F I

G 0 9 C 1/00

G 0 6 F 9/06

H 0 4 L 9/00

6 4 0 B

5 5 0 Z

6 7 5 D

審査請求 未請求 請求項の数24 O L (全 17 頁)

(21) 出願番号 特願平9-342543

(22) 出願日 平成9年(1997)12月12日

(31) 優先権主張番号 特願平9-15079

(32) 優先日 平9(1997)1月29日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 笥 るみ子

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

(72) 発明者 齊藤 和雄

神奈川県足柄上郡中井町境430 グリーン

テクなかい 富士ゼロックス株式会社内

(74) 代理人 弁理士 澤田 俊夫

(54) 【発明の名称】 ユーザ認証装置および方法

(57) 【要約】

【課題】 ユーザ認証手順において、デジタル知財に固有な情報や、デジタル知財側で記録された情報などの付属情報を安全に証明装置へ送信し、かつ、前記送信の過程において送信される付属情報をユーザが確認できる。

【解決手段】 付属情報記憶部11は、送信対象の付属情報を記憶する。試験情報生成部12は、認証用データおよび付属情報の組から試験情報を生成する。試験情報送信部13は、試験情報と、付属情報とを、証明装置30に送信する。証明装置30の試験情報受信部31は、試験情報と付属情報の対を受信し、証明データ生成部32は、試験情報および付属情報から証明データを生成する。付属情報格納部34では、付属情報をICカードに記録する。検証装置30の証明データ受信部14は、証明データを受信し、検証用演算部15は、証明データを検証する。

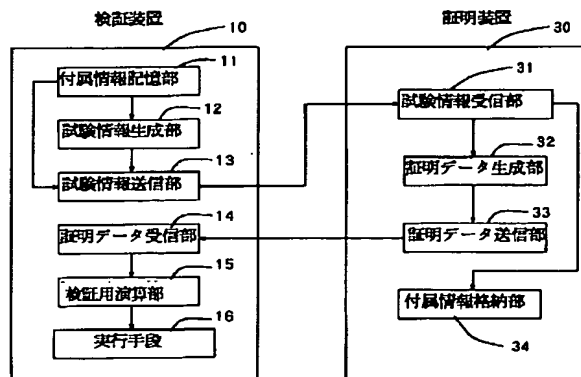


図1

**【特許請求の範囲】**

【請求項1】 ユーザの権限を証明するために生成された証明用データの正当性を検証することにより、上記ユーザの権限を認証するユーザ認証装置において、認証用データを記憶する第1の記憶手段と、デジタル知財の付属情報を記憶する第2の記憶手段と、上記第1の記憶手段に保持されている認証用データと、上記第2の記憶手段に保持されているデジタル知財の付属情報とに所定の演算を施して試験情報を生成する試験情報生成手段と、上記試験情報生成手段によって生成された試験情報と上記第2の記憶手段に記憶されている上記付属情報とに所定の演算を施して証明データを生成する証明データ生成手段と、

上記証明データ生成手段によって生成された証明データに所定の演算を施して正当性の検証を行う証明データ検証手段とを有することを特徴とするユーザ認証装置。

【請求項2】 ユーザ認証用の秘密情報を記憶する第3の記憶手段を有し、上記試験情報生成手段は、上記1の記憶手段に保持されている認証用データと、上記第2の記憶手段に保持されているデジタル知財の付属情報とに所定の演算を施して試験情報を生成し、

上記証明データ生成手段は、上記試験情報生成手段によって生成された試験情報と、上記第2の記憶手段に記憶されている上記付属情報と、上記第3の記憶手段に記憶されている上記秘密情報とに所定の演算を施して証明データを生成することを特徴とする請求項1記載のユーザ認証装置。

【請求項3】 ユーザの固有情報を記憶する第4の記憶手段と、

上記ユーザの固有情報と上記秘密情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第5の記憶手段とを有し、

上記試験情報生成手段は、上記1の記憶手段に保持されている認証用データと、上記第2の記憶手段に保持されているデジタル知財の付属情報とに所定の演算を施して試験情報を生成し、

上記証明データ生成手段は、上記試験情報生成手段によって生成された試験情報と、上記第2の記憶手段に記憶されている付属情報と、上記第4の記憶手段に記憶されているユーザの固有情報と、上記第5の記憶手段に記憶されている上記証明用補助情報とに所定の演算を施して証明データを生成し、

上記証明データ検証手段は、上記証明データが上記ユーザの固有情報に基づいて生成されていることを検証することを特徴とする請求項1記載のユーザ認証装置。

【請求項4】 上記証明データ生成手段が、第1の演算手段と、第2の演算手段とから構成され、第1の演算手段は、上記試験情報生成手段によって生成

された試験情報と、上記第5の記憶手段に記憶されている上記証明用補助情報とに所定の計算を施し、第2の演算手段は、上記第1の演算手段による計算結果と、上記第2の記憶手段に記憶されている付属情報と、上記第4の記憶手段に記憶されているユーザの固有情報とに所定の計算を施し、その結果として上記証明データを生成することを特徴とする請求項3記載のユーザ認証装置。

【請求項5】 認証用データを記憶する第1の記憶手段と、デジタル知財の付属情報を記憶する第2の記憶手段と、第2の記憶手段に記憶されている上記付属情報と上記第1の記憶手段に記憶されている上記認証用データとに基づいて試験情報を生成する試験情報生成手段と、対応する証明装置が生成した上記証明データを記憶する第6の記憶手段と、上記第6の記憶手段に記憶されている上記証明データを検証する証明データ検証手段とを有することを特徴とする検証装置。

【請求項6】 上記試験情報を生成する上記試験情報生成手段は、上記付属情報と上記認証用データとを、上記付属情報を利用しなければ分離不可能な形式で結合して暗号化を行い、上記試験情報を生成することを特徴とする請求項5記載の検証装置。

【請求項7】 ユーザ認証の秘密情報を記憶する第3の記憶手段と、対応する検証装置が生成した試験情報を記憶する第7の記憶手段と、

デジタル知財の付属情報を記憶する第8の記憶手段と、上記第7の記憶手段に記憶されている上記試験情報と上記第8の記憶手段に記憶されている上記付属情報と上記第3の記憶手段に記憶されている上記秘密情報とに所定の演算を施して、証明データを生成する証明データ生成手段とを有することを特徴とする証明装置。

【請求項8】 ユーザの固有情報を記憶する第4の記憶手段と、証明用補助情報を記憶する第5の記憶手段と、対応する検証装置が生成した試験情報を記憶する第7の記憶手段と、

デジタル知財の付属情報を記憶する第8の記憶手段と、上記第4の記憶手段に記憶されている上記ユーザの固有情報と、上記第5の記憶手段に記憶されている上記証明用補助情報と、上記第7の記憶手段に記憶されている上記試験情報と、上記第8の記憶手段に記憶されている上記付属情報とに所定の演算を施して、証明データを生成する証明データ生成手段とを有することを特徴とする証明装置。

【請求項9】 検証装置が、少なくとも、認証用データを記憶する第1の記憶手段と、デジタル知財の付属情報を記憶する第2の記憶手段と、第2の記憶手段に記憶さ

れている上記付属情報と上記第1の記憶手段に記憶されている上記認証用データとに基づいて試験情報を生成する試験情報生成手段と、証明装置が生成した上記証明データを記憶する第6の記憶手段と、上記第6の記憶手段に記憶されている上記証明データを検証する証明データ検証手段とを具備し、上記証明装置が、少なくとも、上記検証装置が生成した試験情報を記憶する第7の記憶手段と、デジタル知財の付属情報を記憶する第8の記憶手段と、上記第7の記憶手段に記憶されている上記試験情報と上記第8の記憶手段に記憶されている上記付属情報とに所定の演算を施して、証明データを生成する証明データ生成手段とを具備し、上記検証装置と上記証明装置とが、互いに通信することによりユーザを認証するユーザ認証装置において、

上記検証装置は、上記試験情報生成手段により生成された試験情報を上記証明装置の上記第7の記憶手段に書き出し、

さらに、上記第2の記憶手段に記憶されている上記付属情報を上記証明装置の上記第8の記憶手段に書き出し、上記証明装置は、上記試験情報生成手段によって上記第7の記憶手段に書き込まれた上記試験情報と、上記第8の記憶手段に書き込まれた上記付属情報とをもとにして上記証明データ生成手段により生成された証明データを上記検証装置の上記第6の記憶手段に書き出し、上記検証装置は、上記第6の記憶手段に書き込まれた上記証明データを用いてユーザを認証することを特徴とするユーザ認証装置。

【請求項10】 上記検証装置から上記証明装置に書き出される付属情報をユーザが確認し、上記デジタル知財の利用中止を決定することが可能な請求項9記載のユーザ認証装置。

【請求項11】 上記検証装置から上記証明装置に書き出される付属情報が故意または事故のため改変あるいは損傷した場合、上記証明装置で生成される証明データが不正なものとなり、上記検証装置において上記デジタル知財の利用禁止の決定を行うことが可能な請求項9乃至10記載のユーザ認証装置。

【請求項12】 上記検証装置から上記証明装置に上記試験情報と上記付属情報とを書き出した後、何らかの理由により、上記検証装置が上記証明装置からの証明データを書き出すことが不可能だった場合、上記検証装置において上記デジタル知財の利用禁止の決定を行うことが可能な請求項9乃至11記載のユーザ認証装置。

【請求項13】 上記デジタル知財の付属情報が、デジタル知財を識別するための識別子であることを特徴とする請求項1乃至12記載のユーザ認証装置。

【請求項14】 上記デジタル知財の付属情報が、デジタル知財の利用履歴であることを特徴とする請求項1乃至12記載のユーザ認証装置。

【請求項15】 上記デジタル知財の付属情報が、デジ

タル知財の利用履歴を、非衝突性関数の入力として計算した値であることを特徴とする請求項1乃至12記載のユーザ認証装置。

【請求項16】 認証用の検証装置において、デジタル知財の付属情報とユーザの認証を行うための認証用データとに基づいて試験情報を生成するステップと、上記認証用の検証装置から認証用の証明装置へ、上記付属情報とともに上記試験情報を送信するステップと、送信された上記付属情報を格納するステップと、上記付属情報および上記試験情報から証明データを生成するステップと、生成された上記証明データを上記検証装置において検証するステップとを有することを特徴とするユーザ認証方法。

【請求項17】 上記検証装置から上記証明装置に送信される付属情報をユーザが確認し、デジタル知財の利用中止を決定することが可能な請求項16記載のユーザ認証方法。

【請求項18】 上記検証装置における検証が失敗した時に上記デジタル知財の利用を禁止する請求項16乃至17記載のユーザ認証方法。

【請求項19】 上記検証装置から上記証明装置に上記試験情報および上記付属情報が送信された後、上記検証装置が上記証明装置からの証明データを受信しない場合、上記デジタル知財の利用を禁止する請求項16乃至18記載のユーザ認証方法。

【請求項20】 上記検証装置から上記証明装置に上記試験情報および上記付属情報とともに、認証を行うために必要な証明用補助情報を送信し、上記証明装置は上記検証装置から送信された上記付属情報と上記証明用補助情報と上記証明装置で保持しているユーザ固有の情報とを用いて上記試験情報から証明データを生成し、上記検証装置に送信して認証を行う請求項19記載のユーザ認証方法。

【請求項21】 デジタル知財管理部側で生成された付属情報を上記デジタル知財管理部側からユーザアクセス可能領域へ送信するユーザ認証方法において、上記デジタル知財管理部側で生成された付属情報とユーザの認証を行うための認証用データとに基づいて、上記デジタル知財管理部側に設けられた認証用の検証装置において試験情報を生成するステップと、上記認証用の検証装置から認証用の証明装置へ上記試験情報を送信するステップと、上記付属情報を上記ユーザアクセス可能領域および上記証明装置へ送信するステップと、送信された上記付属情報を格納するステップと、上記付属情報および上記試験情報から証明データを生成するステップと、生成された上記証明データを上記検証装置において検証

するステップとを有することを特徴とするユーザ認証方法。

【請求項22】 上記デジタル知財の付属情報が、デジタル知財を識別するための識別子であることを特徴とする請求項16乃至21記載のユーザ認証方法。

【請求項23】 上記デジタル知財の付属情報が、デジタル知財の利用履歴であることを特徴とする請求項16乃至21記載のユーザ認証方法。

【請求項24】 上記デジタル知財の付属情報が、デジタル知財の利用履歴を、非衝突性関数の入力として計算した値であることを特徴とする請求項16乃至21記載のユーザ認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ユーザの権限を証明するために生成された証明用データの正当性を検証することにより、上記ユーザの権限を認証するユーザ認証技術において、デジタル知財側に固有な情報や、デジタル知財側で記録された情報などの付属情報を安全に証明装置へ送信し、かつ、送信の過程で、送信される付属情報をユーザが検証することが可能なユーザ認証技術に関する。

【0002】

【従来の技術】デジタル情報は、その複写にかかるコストがほぼゼロであり、かつ、元の情報と全く同一のコピーが得られるという特徴を持つ。したがって、コンピュータソフトウェアやマルチメディアタイトルを始めとするデジタル知財（財産的価値を有するデジタル情報）に対する著作権を保護するためには、その利用を制御する仕組みが必要となる。

【0003】そのための仕組みとして、デジタル知財の一部または全部を暗号化し、正当な権利を持つユーザのみが復号することができるようにすることで、デジタル知財の利用を制御するというアクセス制御の方法がある。これによって、悪意のあるユーザが不正にデジタル知財をコピーしても、それを利用することを防止することができる。つまり、デジタル知財の復号鍵の配布を制御することで、デジタル知財の利用を制御できるのである。

【0004】上記の要求を満たすアクセス制御の一例として、「デジタル著作物流通の為のアクセス制御スキーム」、電子情報通信学会技術報告ISEC97-20（1997-07）、1997年（申吉浩、小島俊一）の論文で提案された手法がある。この論文で述べられている方法では、以下のようにアクセス制御を行う。

【0005】各ユーザは、ユーザ毎に異なる固有の情報を、ICカード等の耐タンパー特性を有する、トークンと呼ばれるハードウェア内に保持し、アクセス権付与者は、特定のデジタル知財に対するアクセス権を、ユーザの固有情報毎にカスタマイズされたアクセスチケットと

呼ばれる形で配布する。この方法では、暗号化されたデジタル知財の復号鍵を直接配布することがないので、復号鍵を不正にコピーされることはない。また、正しいユーザの固有情報とアクセスチケットとの組を持つユーザだけが、そのデジタル知財にアクセスすることができるので、他人のアクセスチケットをコピーしても、デジタル知財の復号を行うことはできず、不正利用を防ぐことができる。また、アクセスチケットの有効期限の判定や利用履歴の保持などの、安全性を要する処理は、すべてトークン内で行われるので、情報の改竄や詐称を行うことはできない。

【0006】以上の論文の手法によって、デジタル知財に対するユーザ単位のアクセス制御の実現が可能になった。さらに、デジタル知財の復号の履歴を、使用したアクセスチケットの情報と共にトークンに記録し、適当なタイミングで課金業者による履歴の回収を行うことによって、デジタル知財の利用に応じて課金する、いわゆる、利用量課金も行えるようになった。

【0007】

【発明が解決しようとする課題】上述の論文の手法による利用量課金は、アクセスチケットの利用履歴を記録することによって実現されることになる。しかしながら、この方法では、以下に示すような種類の履歴を記録することができない。これは利用量課金の多様性を阻害する要因となるものである。

【0008】①同一のアクセス権（アクセスチケット）を用いて、複数の異なるデジタル知財の利用を制御する場合、制御対象のデジタル知財毎に固有な情報を履歴として記録することができない。

②デジタル知財の利用時に決まる様な種類の利用履歴を記録することができない。

【0009】これらについて、以下で詳細に説明する。

【0010】①について

上述の論文の手法では、アクセス権（アクセスチケット）に固有の情報については、履歴としてトークンに記録できる様な仕組みが提供されている。したがって、特定のソフトウェアが特定のアクセス権（アクセスチケット）に対応づけられていれば、アクセスチケットの固有情報を記録することで、目的を達成することが可能である。しかし、ある特定のアクセスチケットを用いて複数のデジタル知財の利用を制御する場合には、その仕組みを用いることができない。たとえば、あるアクセスチケットAで、アプリケーションソフトウェアaとbという二つの種類が使用できるものとする。この場合、履歴として記録できるのはアクセスチケットAを使用したという履歴のみであり、アプリケーションソフトウェアaあるいはbのどちらのアプリケーションソフトウェアを利用したのかという履歴を記録することはできないのである。

【0011】このような問題は、たとえばアプリケーシ

ョンプログラムのバージョンアップ時などに顕著に表れる。バージョンアップにおいては、アプリケーションの作成者側にとって、バージョンアップ毎にアクセス権の配布を行わなくて済み、またユーザにとっては、新たなアクセスチケットを取得することなく新バージョンのアプリケーションを使いつづけられるため、同一のアクセスチケットで、異なるバージョンのソフトウェアの利用制御を行えることが望ましい。しかし、古いバージョンと新しいバージョンとでその1回の利用料金に差をつけるなどの処理を実施するためには、ユーザが用いたバージョンを履歴として記録する必要があることになる。

#### 【0012】②について

また、上述の論文の手法では、デジタル知財の利用履歴も、復号時にしか記録することができない。復号を行った履歴を記録するだけでは、そのデジタル知財の利用回数しか測定することができず、複数の機能を包含するアプリケーションプログラムのようなデジタル知財については、利用されたことのみを履歴として記録できるだけで、そのアプリケーションプログラムの利用機能や利用状況に応じた履歴を記録することはできない。たとえば、ワードプロセッサのようなアプリケーションプログラムの場合、編集開始時の対象文書のデータ量と編集終了時のそのデータ量との差、あるいは対象文書に対して行った操作の総量といった利用量に対する課金は、復号の履歴では行うことができない。詳細な履歴を記録するためには、復号時ではなくアプリケーションプログラムの利用時に利用量の測定を行わなければならない。このためには、デジタル知財側で利用量を測定する必要がある。

【0013】上記の課題を解決するためには、デジタル知財の識別子や測定された利用量などの、デジタル知財側にある情報を、記録するための媒体であるトークンに伝達する必要がある。これらの情報は、悪意のあるユーザによる改竄を防ぐため、安全にトークンへ伝達されなければならない。

【0014】一方、安全に情報を伝達する方法の例としては、特公平07-118709号公報がある。特公平07-118709号公報では、証明用秘密データを入力とした一方向性関数値を、公開データとしてあらかじめ公開しておく。受信側が公開データを入手した後、送信側は、秘密情報と認証用秘密データとを連結して暗号化した値を受信側に送信する。受信側では、送られたデータを復号して認証用秘密データの一方向性関数値を計算し、公開データと比較することで、送信データの正当性を検証する。

【0015】しかしながら、特公平07-118709号公報を用いた場合、履歴情報は秘密情報として送信されることになり、デジタル知財の利用者は、検証側から証明側へどのような履歴が送付されているのかを知るすべがない。

【0016】記録される履歴情報は、利用量課金の原データとなるので、利用者に対して隠蔽することは望ましくない。悪意のある検証装置が、高価な利用履歴を捏造して送信したり、あるいは事故によって、不当に高い利用履歴が送信されてしまったりする可能性があるためである。

【0017】したがって、検証側から送付される履歴はユーザが確認可能な形態でなければならない。さらに、ユーザが不信に思った場合は、履歴の送付を中断できるような機構を設けることが望ましい。

【0018】本発明は、上記の課題を解決するためになされたもので、デジタル知財に固有な情報や、デジタル知財側で記録された情報などの付属情報を安全に証明装置へ送信することが可能であり、かつ、前記送信の過程において送信される付属情報をユーザが確認することが可能なユーザ認証装置を提供することを目的とする。

#### 【0019】

【課題を解決するための手段】本発明のユーザ認証装置は、ユーザの権限を証明するために生成された証明用データの正当性を検証することにより、上記ユーザの権限を認証するユーザ認証装置において、認証用データを記憶する第1の記憶手段と、デジタル知財の付属情報を記憶する第2の記憶手段と、上記第1の記憶手段に保持されている認証用データと、上記第2の記憶手段に保持されているデジタル知財の付属情報とに所定の演算を施して試験情報を生成する試験情報生成手段と、上記試験情報生成手段によって生成された試験情報と上記第2の記憶手段に記憶されている上記付属情報とに所定の演算を施して証明データを生成する証明データ生成手段と、上記証明データ生成手段によって生成された証明データに所定の演算を施して正当性の検証を行う証明データ検証手段とを有することを特徴とする。

#### 【0020】

【発明の実施の態様】以下、本発明の実施例を説明する。本実施例は、暗号化されたアプリケーションプログラムを、パソコンやワークステーションなどの情報処理装置で利用し、利用機能や利用時間等の利用量、アプリケーションプログラムの識別子や使用価格などを、その情報処理装置に接続したICカードに記録するシステムである。

【0021】図1は、本発明の構成例を示している。この構成例の各部は、以下の各実施例に共通するので、実施例1の説明においてまとめて説明することにする。

【0022】【実施例1】実施例1では、本発明を、ユーザのPC（パーソナルコンピュータ）あるいはワークステーション上で動作するアプリケーションプログラムの実行制御に用い、アプリケーションプログラムの識別子を付属情報としてICカードに送信する場合について述べる。

#### 【0023】暗号化されたアプリケーションプログラム

は、検証装置によって管理されており、アプリケーションプログラムの識別子は、証明装置で管理されているICカードに送信され、記録される。

【0024】図1において、検証装置10は、付属情報記憶部11、試験情報生成部12、試験情報送信部13、証明データ受信部14、検証用演算部15、実行手段16を含んで構成され、一定時間毎や、使用しているアプリケーションプログラムに内在する特定の機能を起動した瞬間などの任意のタイミングで、試験情報を生成し、証明装置30に対して送信する。アプリケーションの識別子を送信する際、試験情報生成部12では、認証データCと、アプリケーションの識別子Iとを組み合わせ、暗号化して試験情報Tを生成する。また、証明装置30は、試験情報受信部31、証明データ生成部32、証明データ送信部33、付属情報格納部34を含んで構成され、検証装置10から送られてきた試験情報T等に基づいて証明情報を生成し、検証装置10に返す。また検証装置10から送られてきた識別子Iを付属情報格納部34に格納する。

【0025】ここでは、認証にRSA(Rivest-Shamir-Adleman)暗号を用いた場合について説明する。

【0026】図2に検証装置10の構成を示す。図2において、付属情報記憶部11では、アプリケーションプログラムの識別子を記憶している。試験情報生成部12は、乱数生成部17、認証用データ生成部18、検証用情報Kを記憶する検証用情報記憶部19、RSA公開鍵(E, n)を記憶する公開鍵記憶部20からなり、証明装置30に送信する試験情報Tを生成する。

【0027】試験情報送信部13は、試験情報生成部12で生成した試験情報Tと暗号化していない識別子Iとの対を、証明装置30に送信する。証明データ受信部14は、証明装置30から送られてきた証明データを受信し、検証用演算部15へ渡す。検証用演算部15は、証明装置30から受信した証明データを検証し、正しければ、アプリケーションプログラムを復号して実行手段16に渡し、実行する。

【0028】図3に、証明装置30の構成を示す。図3において、証明装置30は、試験情報受信部31、証明データ生成部32、証明データ送信部33、付属情報格納部34、RSA秘密鍵D/法数nを記憶する秘密鍵記憶部35から構成される。

【0029】試験情報受信部31は、検証装置10から送信された試験情報Tと識別子Iの対を受信する。証明データ生成部32では、受信した試験情報Tと暗号化されていない識別子I、RSA秘密鍵D/法数nを用いて試験情報から証明データを生成する。証明データ送信部33は、証明データ生成部32で生成された証明データを検証装置10に送信する。

【0030】付属情報格納部34では、試験情報と共に

受信した暗号化されていない識別子IをICカードに記録する。

【0031】証明装置30のRSA秘密鍵記憶部35に保持されているRSA秘密鍵をD、公開鍵ペアを(E, n)とする。

【0032】図4に、処理の流れを示す。

【0033】[ステップ1] 検証装置10では、乱数生成部17で乱数rを生成し、認証用データ生成部18で認証用データC

【0034】

【数1】 $C = rK \bmod n$

を生成する。

【0035】[ステップ2] ステップ1で生成された認証用データCと識別子Iを結合し、公開鍵Eで暗号化して試験情報Tを生成する。

【0036】

【数2】 $T = (C + I)^E \bmod n$

【0037】[ステップ3] 検証装置10の試験情報送信部13は、試験情報Tおよび暗号化されていない識別子Iを証明装置30に送信する。

【0038】[ステップ4] 証明装置30の試験情報受信部31は、検証装置10から送信された試験情報Tおよび暗号化されていない識別子Iを受信し、証明データ生成部32に渡す。

【0039】[ステップ5] 証明装置30の証明データ生成部32は、受信したTを秘密鍵Dで復号する。

【0040】

【数3】 $T' = T^D \bmod n$

【0041】[ステップ6] 更に、検証装置10から送信された暗号化されていない識別子Iを用いてT'からIを取り除き、証明データRを生成する。

【0042】

【数4】 $R = (T' - I) \bmod n$

【0043】[ステップ7] 証明装置30の証明データ送信部33は、生成した証明データRを検証装置10に送信する。

【0044】[ステップ8] 証明装置30の付属情報格納部34は、識別子IをICカードに記録する。

【0045】[ステップ9] 検証装置10の証明データ受信部14は、証明データRを受け取り、検証用演算部15で以下のようにK'を生成し、検証用情報Kと比較して検証を行う。

【0046】

【数5】 $K' = r^{-1}R \bmod n$

【0047】[ステップ9'] 一定時間、証明データRが返ってこなかった場合、検証装置10は認証に失敗したと判断し、アプリケーションプログラムの利用を中止する。

【0048】[ステップ10] ステップ9の結果、KとK'が等しければ認証は成功し、アプリケーションプ

プログラムの復号および実行を行う。そうでなければ、アプリケーションプログラム利用の続行を中止する。

【0049】ユーザは、ステップ3の過程で送信される識別子Iを調べ、この段階で識別子の送信を中止することができる。この場合、検証装置10には証明データRが返ってこないで、認証に失敗し、アプリケーションプログラムの利用は中止される。また、ここで識別子Iを改竄した場合、ステップ1の過程で生成される認証用データCが不正なものとなり、認証に失敗する。

【0050】識別子のような、デジタル知財に固有の情報を伝達することは、利用量課金だけでなく、アクセス制御にも有用な効果を及ぼす。たとえば、各ユーザに与えられたアクセス権の有効期限とは別に、デジタル知財自体にも有効期限を設けておき、証明装置では送られてきた有効期限を検査して利用の可否を決定するように装置を構成することができる。このような構成にすることで、ユーザ単位のアクセス制御と、デジタル知財単位のアクセス制御とを併用することができる。

【0051】〔実施例2〕実施例2では、アプリケーションプログラムの利用履歴を付属情報としてICカードに送信する場合について述べる。

【0052】通常、アプリケーションプログラムで使用機能や時間等の履歴を記録する場合、その記録量は相当多量となることが想定される。本発明では、認証用データと付属情報とを結合して暗復号を行うため、暗復号に要する時間が付属情報の大きさに左右される。

【0053】また、送信する履歴のフォーマットは、多種多様なものが考えられるので、どのようなフォーマットでも扱えるような方法が望ましい。

【0054】そのために本実施例では、検証装置と証明装置で同じ方向ハッシュ関数を持たせ、認証用データと結合する付属情報に、この出力を利用することとする。

【0055】一方方向ハッシュ関数とは、 $h(x) = h(y)$ を満たす異なる $x$ 、 $y$ を算出することが著しく困難であるという性質をもつ関数である。一方方向ハッシュ関数の例として、RSA Data Security Inc. によるMD2、MD4、MD5、米国連邦政府による規格SHS (Secure Hash Standard) が知られている。

【0056】図5に検証装置10の構成を示す。図5において、付属情報記憶部11では、アプリケーションプログラムの利用量を記録している。

【0057】試験情報生成部12は、乱数生成部17、認証用データ生成部18、ハッシュ値生成部21、検証用情報Kを記憶する検証用情報記憶部19、RSA公開鍵(E, n)を記憶する公開鍵記憶部20からなり、証明装置30に送信する試験情報Tを生成する。

【0058】試験情報送信部13は、試験情報生成部12で生成した試験情報Tと、暗号化されていない利用履

歴udの対を、証明装置30に送信する。

【0059】証明データ受信部14は、証明装置30から送られてきた証明データRを受信し、検証用演算部15へ渡す。検証用演算部15は、証明装置30から受信した証明データRを検証し、正しければ、アプリケーションプログラムを復号して実行手段16に渡し、実行する。

【0060】図6に証明装置の構成を示す。図6において、証明装置30は、試験情報受信部31、ハッシュ値生成部36、証明データ生成部32、証明データ送信部33、付属情報格納部34、RSA秘密鍵D/法数nを記憶する秘密鍵記憶部35から構成される。

【0061】試験情報受信部31は、検証装置10から送信された試験情報Tと利用履歴udの対を受信する。ハッシュ値生成部36では、受信した利用履歴udを入力とするハッシュ値を生成する。証明データ生成部32では、受信した試験情報Tとハッシュ値生成部36で生成されたハッシュ値、RSA秘密鍵D/法数nを用いて試験情報Tから証明データRを生成する。証明データ送信部33は、証明データ生成部32で生成された証明データRを検証装置10に送信する。

【0062】付属情報格納部34では、試験情報と共に受信した暗号化されていない利用履歴udをICカードに記録する。

【0063】証明装置30のRSA秘密鍵記憶部35に保持されているRSA秘密鍵をD、公開鍵ペアを(E, n)とする。

【0064】図7に、処理の流れを示す。

〔ステップ1〕 検証装置10では、乱数生成部17で乱数rを生成し、認証用データ生成部18で認証用データC

【0065】

【数6】 $C = rK \bmod n$

を生成する。

【0066】〔ステップ2〕 さらに、ハッシュ値生成部21で以下の計算を行う。

【0067】

【数7】 $Hash(u_d)$

【0068】〔ステップ3〕 ステップ1で生成された認証用データCとステップ2で生成した値とを結合し、公開鍵Eで暗号化して試験情報Tを生成する。

【0069】

【数8】 $T = (C + Hash(u_d))^E \bmod n$

【0070】〔ステップ4〕 検証装置10の試験情報送信部13は、試験情報Tおよび暗号化されていない利用履歴udを証明装置30に送信する。

【0071】〔ステップ5〕 証明装置30の試験情報受信部31は、検証装置10から送信された試験情報Tおよび暗号化されていない利用履歴udを受信し、証明データ生成部32に渡す。



【0072】[ステップ6] 証明装置30のハッシュ値生成部36は、以下の計算を行い、結果を証明データ生成部32に渡す。

【0073】

【数9】 $\text{Hash}(ud)$

【0074】[ステップ7] 証明装置30の証明データ生成部32は、受信した試験情報Tを秘密鍵Dで復号する。

【0075】

【数10】 $T' = T^D \bmod n$

【0076】[ステップ8] 更に、ハッシュ値生成部36で生成されたハッシュ値を用いて $T'$ から $\text{Hash}(ud)$ を取り除き、証明データRを生成する。

【0077】

【数11】

$R = (T' - \text{Hash}(ud)) \bmod n$

【0078】[ステップ9] 証明装置30の証明データ送信部33は、生成した証明データRを検証装置10に送信する。

【0079】[ステップ10] 証明装置30の付属情報格納部34は、利用履歴udをICカードに記録する。

【0080】[ステップ11] 検証装置10の証明データ受信部14は、証明データRを受け取り、検証用演算部15で以下のように $K'$ を生成し、検証用情報Kと比較して検証を行う。

【0081】

【数12】 $K' = r^{-1}R \bmod n$

【0082】[ステップ11'] 一定時間、証明データRが返ってこなかった場合、検証装置10は認証に失敗したと判断し、アプリケーションプログラムの利用を中止する。

【0083】[ステップ12] ステップ11の結果、Kと $K'$ が等しければ認証は成功し、アプリケーションプログラムの復号および実行を行う。そうでなければ、アプリケーションプログラム利用の続行を中止する。

【0084】ユーザは、ステップ3の過程で送信される利用履歴udを調べ、この段階で履歴の送信を中止することができる。この場合、検証装置10には証明データRが返ってこないため、認証に失敗し、アプリケーションプログラムの利用は中止される。また、ここで利用履歴udを改竄した場合、ステップ1の過程で生成される認証用データCが不正なものとなり、認証に失敗する。

【0085】[実施例3] 次に、上述の論文の認証方法に基づいて利用履歴を送信する実施例を説明する。図8に検証装置10の構成を示し、図9に証明装置30の構成を示す。図8において、22は証明用補助情報(アクセスチケット)tを記憶する証明用補助情報記憶部であり、図9において、37はユーザ固有情報 $d_u$ を記憶するユーザ固有情報記憶部である。

【0086】上述の論文の手法では、ユーザやデジタル知財固有の秘密情報を管理しているセンターを仮定し、ある特定のユーザが特定のデジタル知財にアクセスを行う際、あらかじめセンターからそのデジタル知財固有の情報とユーザ固有の情報とに依存する以下のような証明用補助情報tを生成してもらい、これを用いて認証を行う。

【0087】図10に、処理の流れを示す。なお、証明用補助情報tは例えばつぎのように生成される。

【0088】

【数13】 $t = D - W(n, d_u)$

ここで、 $d_u$ はユーザの固有情報、 $W(x, y)$ は一方方向性関数、p、qは、 $n = pq$ を満たす二つの素数である。証明装置30では秘密鍵D、nは持たず、ユーザの固有情報 $d_u$ を保持している。

【0089】[ステップ1] 検証装置10は、以下のような認証用データCを生成する。

【0090】

【数14】 $C = r^E K^E \bmod n$

【0091】[ステップ2] ステップ1で生成された認証用データCと利用履歴udを結合し、公開鍵Eで暗号化して試験情報Tを生成する。

【0092】

【数15】 $T = (C + ud)^E \bmod n$

【0093】[ステップ3] 検証装置10の試験情報送信部13は、試験情報T、暗号化されていない利用履歴ud、法数n、および証明用補助情報tを証明装置30に送信する。

【0094】[ステップ4] 証明装置30の試験情報受信部31は、検証装置10から送信された試験情報T、暗号化されていない利用履歴ud、法数n、および証明用補助情報tを受信し、証明データ生成部32に渡す。

【0095】[ステップ5] 証明装置30の証明データ生成部32は、受信した試験情報Tをユーザの固有情報 $d_u$ 、証明用補助情報t、法数nを用いて復号する。

【0096】

【数16】 $T' = T(t + W(n, d_u)) \bmod n$

【0097】[ステップ6] 更に、検証装置10から送信された暗号化されていない利用履歴udを用いて $T'$ から利用履歴udを取り除き、ユーザ固有情報 $d_u$ 、証明用補助情報t、法数nを用いて証明データRを生成する。

【0098】

【数17】

$R = (T' - ud)(t + W(n, d_u)) \bmod n$

【0099】[ステップ7] 証明装置30の証明データ送信部33は、生成した証明データRを検証装置10に送信する。

【0100】[ステップ8] 証明装置30の付属情報

格納部34は、利用履歴 $u_d$ をICカードに記録する。

【0101】[ステップ9] 検証装置10の証明データ受信部14は、証明データ $R$ を受け取り、検証用演算部15で以下のように $K'$ を生成し、検証用情報 $K$ と比較し、結果をデジタル知財管理部(実行手段16)に通知する。

【0102】

【数18】 $K' = r^{-1}R \bmod n$

【0103】[ステップ9'] 一定時間、証明データ $R$ が返ってこなかった場合、検証装置10は認証に失敗したと判断し、アプリケーションプログラムの利用を中止する。

【0104】[ステップ10] ステップ9の結果、 $K$ と $K'$ が等しければ認証は成功し、アプリケーションプログラムの復号および実行を行う。そうでなければ、アプリケーションプログラム利用の続行を中止する。

【0105】図11は、検証装置10での処理の流れを示し、図12は証明装置30での処理の流れを示した図である。ステップ7以降は、実施例2と同様の処理を行う。実施例2と同様に、ユーザは、ステップ3の過程で送信される利用履歴 $u_d$ を調べ、この段階で履歴の送信を中止することができる。

【0106】本実施例では、検証装置10が証明用補助情報 $t$ を保持しており、証明装置30に送信するようになっているが、ユーザが証明装置30に与えても良いし、また、最初から証明装置30が維持しているような構成になっていても良い。

【0107】[実施例4] 本実施例では、証明用補助情報 $t$ を利用する、異なった構成の実施例について述べる。

【0108】図13に検証装置10の構成を示し、図14に証明装置の構成を示す。また、図15に、本実施例における処理の流れを示す。証明用補助情報 $t$ は、実施例3と同様に計算される。

【0109】[ステップ1] 検証装置10は、以下のような認証用データを生成する。

【0110】

【数19】 $C = rK \bmod n$

【0111】[ステップ2] ステップ1で生成された認証用データ $C$ と利用履歴 $u_d$ を結合し、公開鍵 $E$ で暗号化して試験情報 $T$ を生成する。

【0112】

【数20】 $T = (C + u_d)^E \bmod n$

【0113】[ステップ3] 検証装置10の試験情報送信部13は、試験情報 $T$ 、暗号化されていない利用履歴 $u_d$ 、法数 $n$ を証明装置に送信する。

【0114】[ステップ4] 証明装置30の試験情報受信部31は、検証装置10から送信された試験情報 $T$ 、暗号化されていない利用履歴 $u_d$ 、法数 $n$ を受信し、証明データ生成部32に渡す。

【0115】[ステップ5] 証明データ生成部32中の第一演算部39は、受信した試験情報 $T$ と証明用補助情報 $t$ を用いて、以下の計算を行い、 $T'$ を得る。

【0116】

【数21】 $T' = T^t \bmod n$

【0117】[ステップ6] 証明データ生成部32中の第二演算部40は、第一演算部39で生成した $T'$ と、ユーザ固有情報 $d_u$ 、法数 $n$ を用いて、以下の計算を行い、 $T''$ を得る。

【0118】

【数22】 $T'' = T' \cdot T^{W(n, d_u)} \bmod n$

【0119】[ステップ7] 証明データ生成部32中の証明データ用演算部41は、検証装置10から送信された暗号化されていない利用履歴 $u_d$ を用いて $T'$ から利用履歴 $u_d$ を取り除き、証明データ $R$ を生成する。

【0120】

【数23】 $R = T' - u_d \bmod n$

【0121】[ステップ8] 証明装置30の証明データ送信部33は、生成した証明データ $R$ を検証装置10に送信する。

【0122】[ステップ9] 証明装置30の付属情報格納部34は、利用履歴 $u_d$ をICカードに記録する。

【0123】[ステップ10] 検証装置10の証明データ受信部13は、証明データ $R$ を受け取り、検証用演算部15で以下のように $K'$ を生成し、検証用情報 $K$ と比較し、結果をデジタル知財管理部(実行手段16)に通知する。

【0124】

【数24】 $K' = r^{-1}R \bmod n$

【0125】[ステップ10'] 一定時間、証明データ $R$ が返ってこなかった場合、検証装置10は認証に失敗したと判断し、アプリケーションプログラムの利用を中止する。

【0126】[ステップ11] ステップ10の結果、 $K$ と $K'$ が等しければ認証は成功し、アプリケーションプログラムの復号および実行を行う。そうでなければ、アプリケーションプログラム利用の続行を中止する。

【0127】図16は、検証装置での処理を示し、図17は証明装置での処理の流れを示した図である。ステップ8以降は、実施例3と同様の処理を行う。実施例3と同様に、ユーザは、ステップ3の過程で送信される利用履歴 $u_d$ を調べ、この段階で履歴の送信を中止することができる。

【0128】本実施例では、証明装置30において、証明用補助情報 $t$ を用いて演算を行う部分と、ユーザの固有情報 $d_u$ を用いて演算を行う部分とが分離している。アプリケーションプログラムの不正利用を防ぐため、ユーザの固有情報およびユーザの固有情報を用いた演算部分は防御する必要があるが、証明用補助情報および証明用補助情報を用いた演算部分は防御する必要がない。こ

のため、本実施例のように演算部分が分離されている場合、ユーザの固有情報に関連する部分の演算はICカード等の防御手段内で行い、それ以外の演算は外部で行うという構成が可能となる。

#### 【0129】

【発明の効果】本発明によれば、デジタル知財側に固有な情報や、デジタル知財側で記録された情報などの付属情報を、安全に証明装置に送信することができる。また、ユーザは、送信される付属情報を検証し、デジタル知財利用の中止を決定することができる。さらに、デジタル知財側で、正しい情報が証明装置に記録されたかどうかを検証し、不正なものが記録された場合にはデジタル知財の利用を禁止することができる。

#### 【図面の簡単な説明】

- 【図1】 実施例の構成を示す図である。  
 【図2】 実施例1における検証装置の構成例を示す図である。  
 【図3】 実施例1における証明装置の構成例を示す図である。  
 【図4】 実施例1の処理の流れを示す図である。  
 【図5】 実施例2における検証装置の構成例を示す図である。  
 【図6】 実施例2における証明装置の構成例を示す図である。  
 【図7】 実施例2の処理の流れを示す図である。  
 【図8】 実施例3における検証装置の構成例を示す図である。  
 【図9】 実施例3における証明装置の構成例を示す図である。  
 【図10】 実施例3の処理の流れを示す図である。  
 【図11】 実施例3における、証明装置に試験情報を送付するまでの検証装置で処理の流れを示す図である。  
 【図12】 実施例3における、証明装置での処理の流れを示す図である。

れを示す図である。

【図13】 実施例4における検証装置の構成例を示す図である。

【図14】 実施例4における証明装置の構成例を示す図である。

【図15】 実施例4の処理の流れを示す図である。

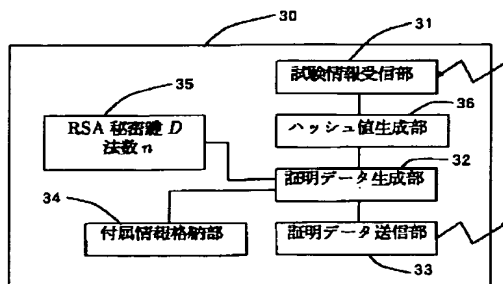
【図16】 実施例4における、証明装置に試験情報を送付するまでの検証装置で処理の流れを示す図である。

【図17】 実施例4における、証明装置での処理の流れを示す図である。

#### 【符号の説明】

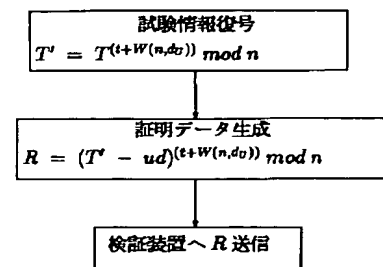
- 10 検証装置
- 11 付属情報記憶部
- 12 試験情報生成部
- 13 試験情報送信部
- 14 証明データ受信部
- 15 検証用演算部
- 16 実行手段
- 17 乱数生成部
- 18 認証用データ生成部
- 19 検証用情報記憶部
- 20 公開鍵記憶部
- 21 ハッシュ値生成部
- 22 証明用補助情報記憶部
- 30 証明装置
- 31 試験情報受信部
- 32 証明データ生成部
- 33 証明データ送信部
- 34 付属情報格納部
- 35 秘密鍵記憶部
- 36 ハッシュ値生成部
- 37 ユーザ固有情報記憶部
- 38 証明用補助情報記憶部

【図6】



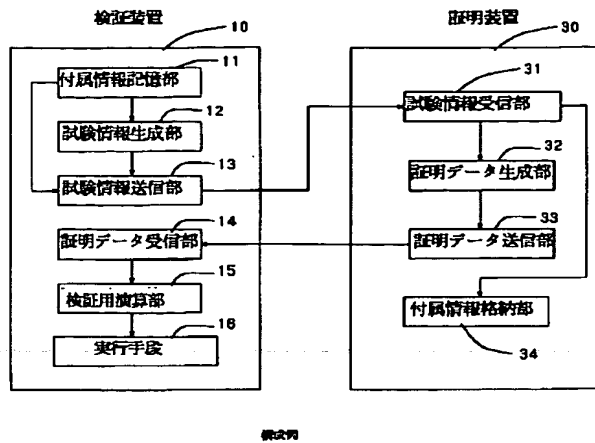
実施例2の証明装置の構成

【図12】



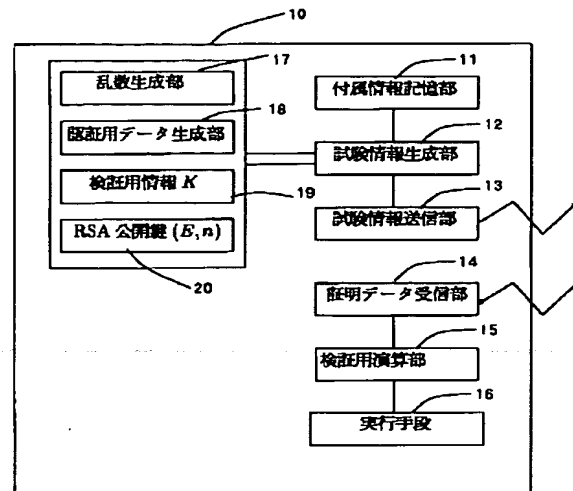
実施例3における証明装置での処理

【図1】



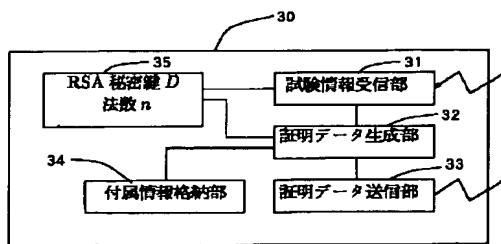
構成例

【図2】



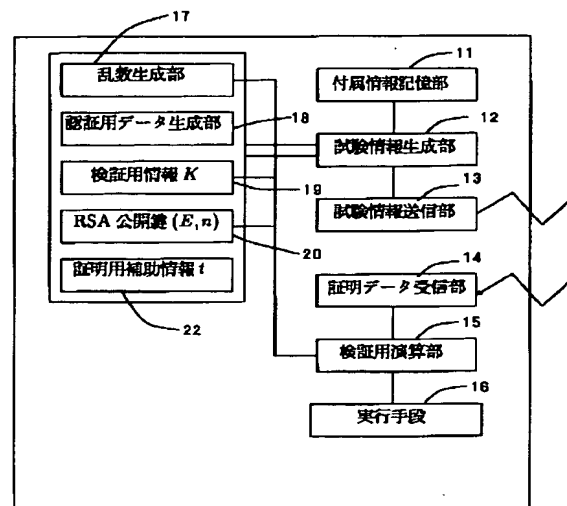
実施例1の検証装置の構成

【図3】



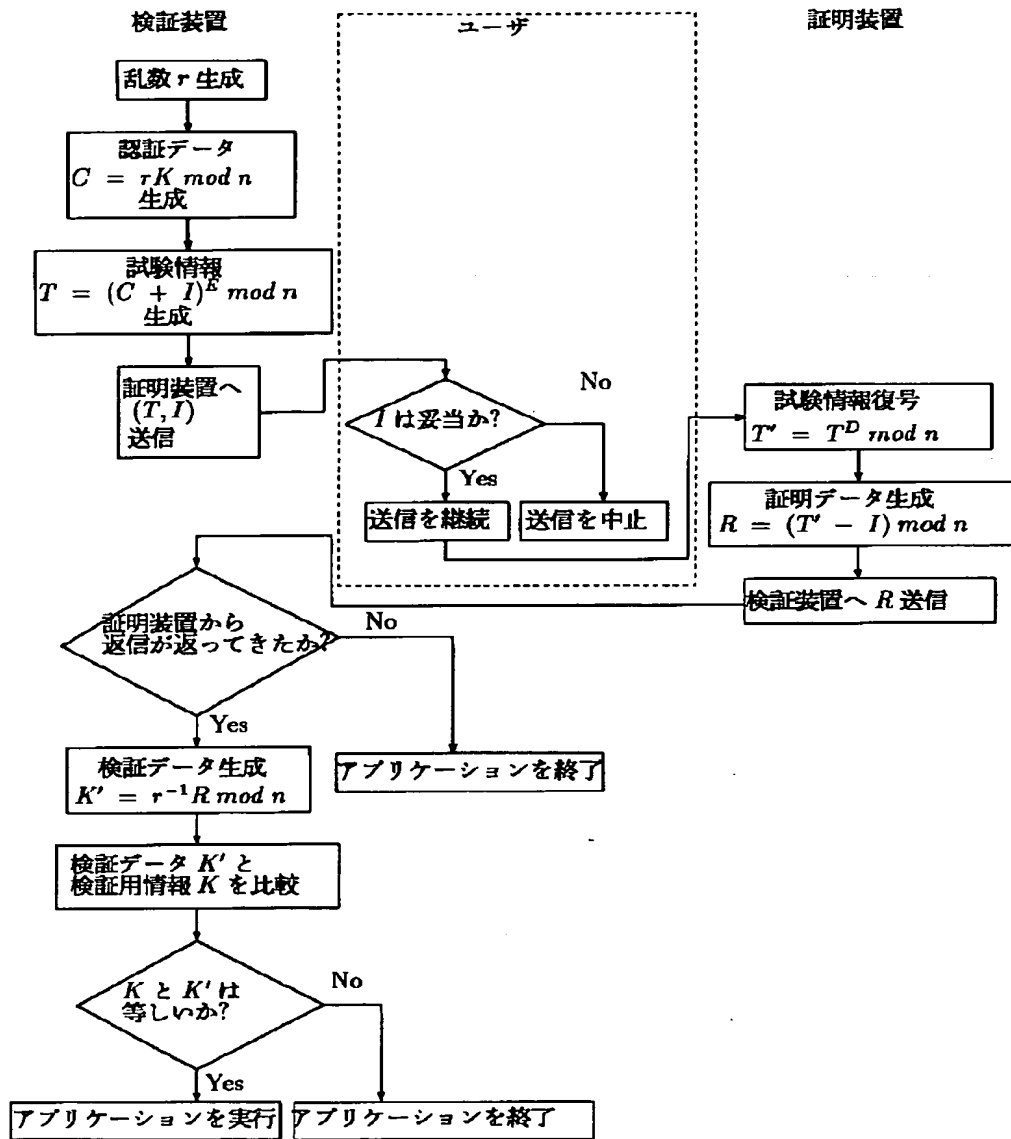
実施例1の証明装置の構成

【図8】



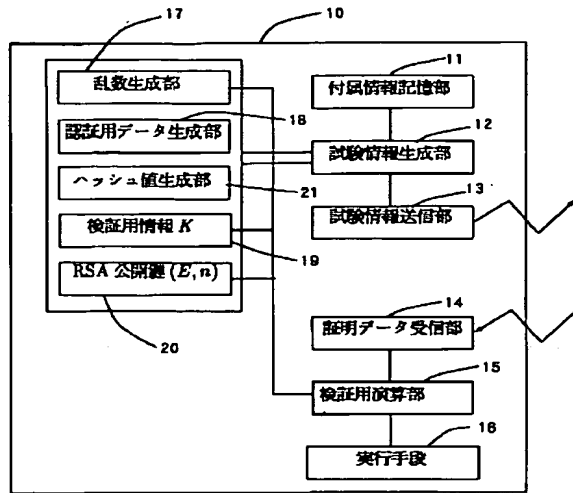
実施例3の検証装置の構成

【図4】



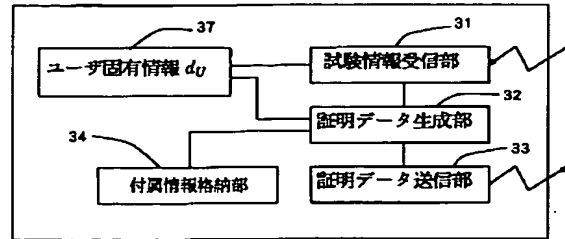
実施例 1 の処理の流れ

【図5】



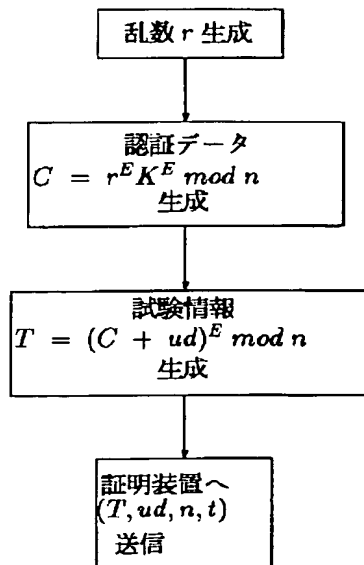
実施例3の検証装置の構成

【図9】



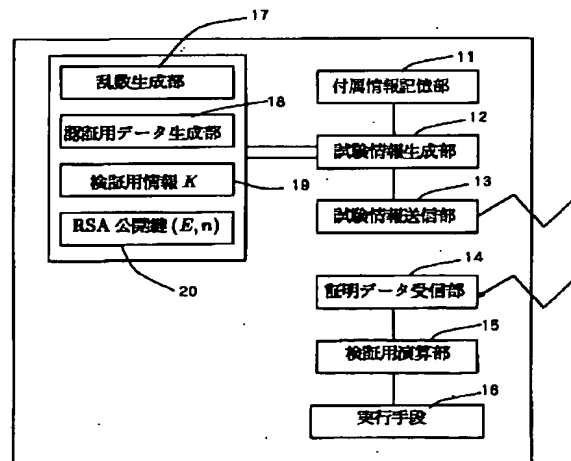
実施例3の証明装置の構成

【図11】



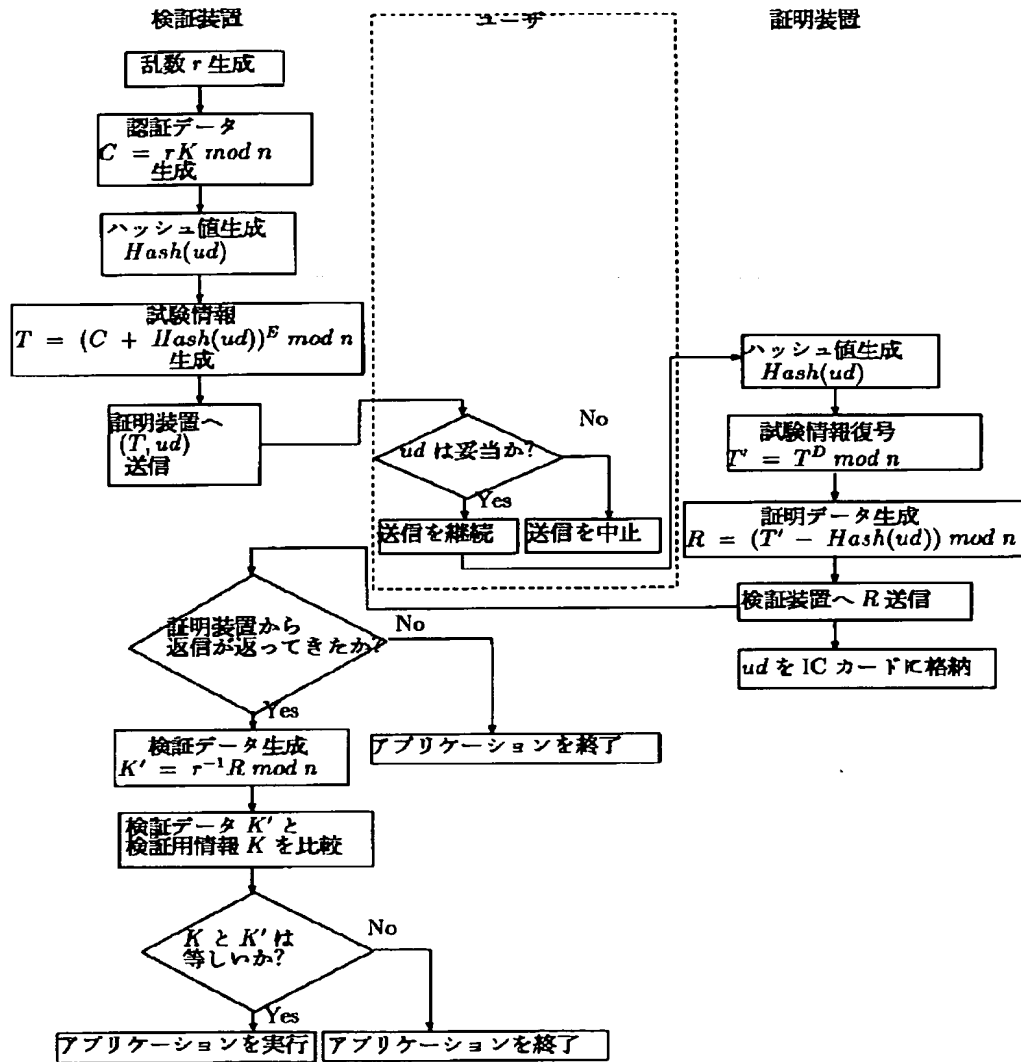
実施例3における検証装置での処理

【図13】



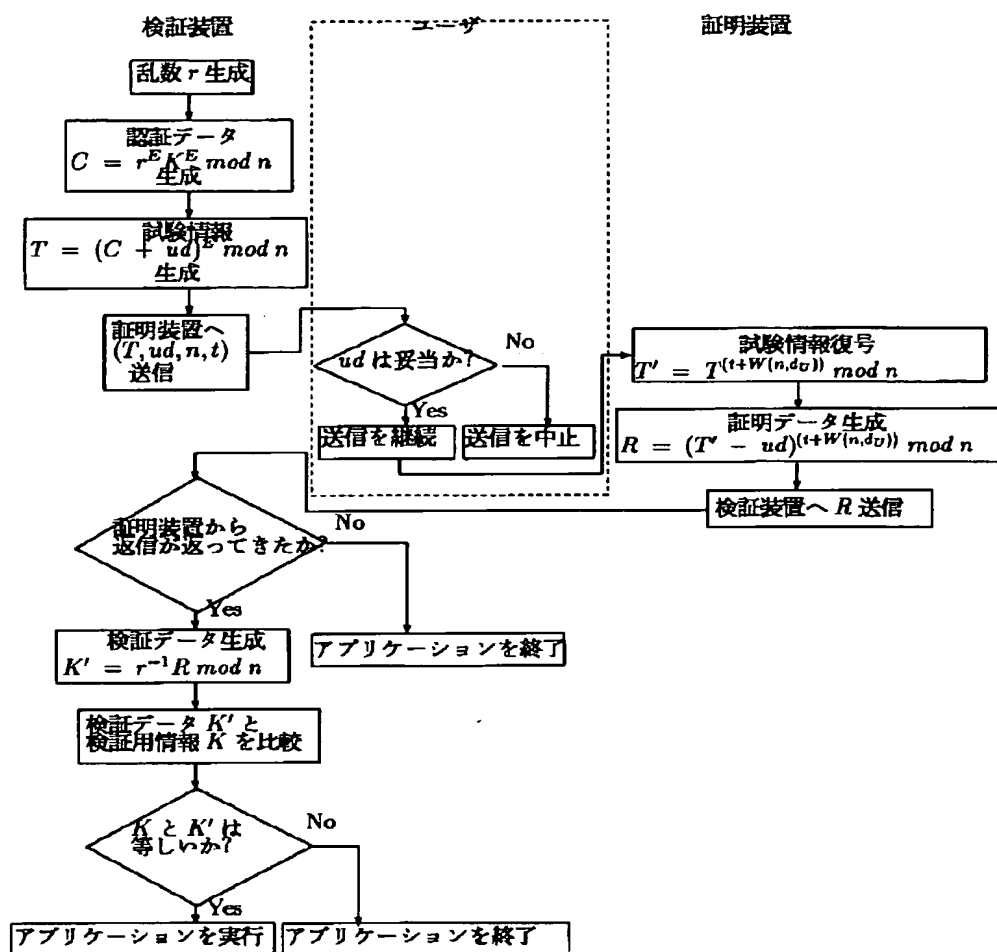
実施例4の検証装置の構成

【図7】



実施例2の処理の流れ

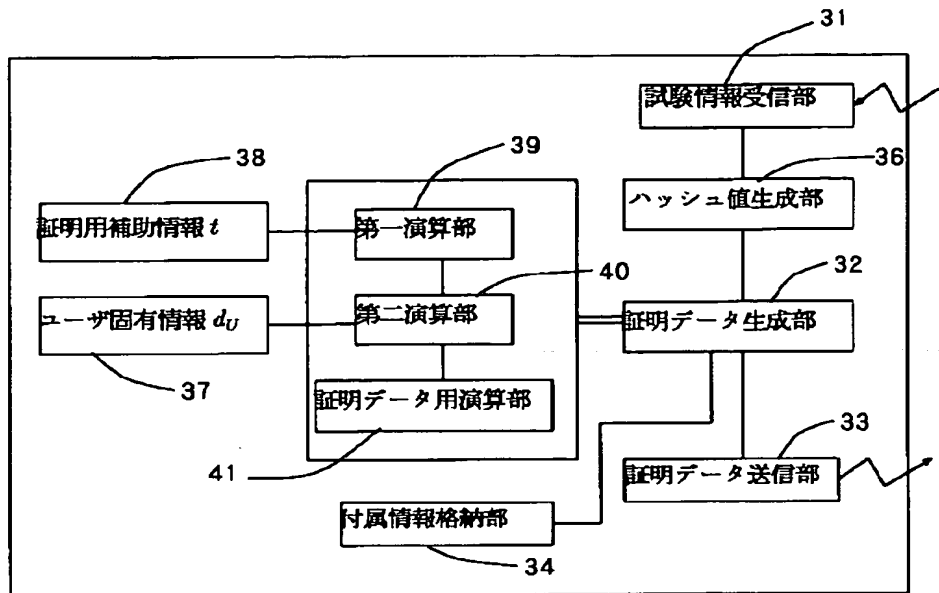
【図10】



実施例 3 の処理の流れ

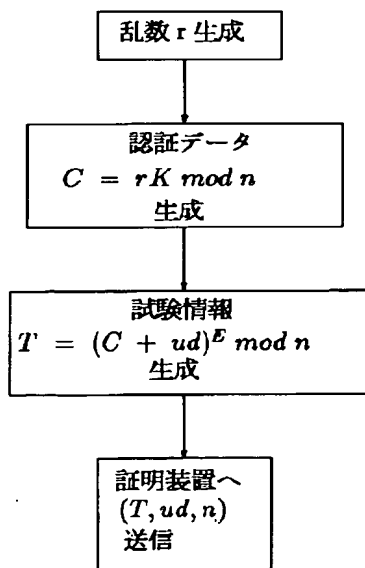


【図14】



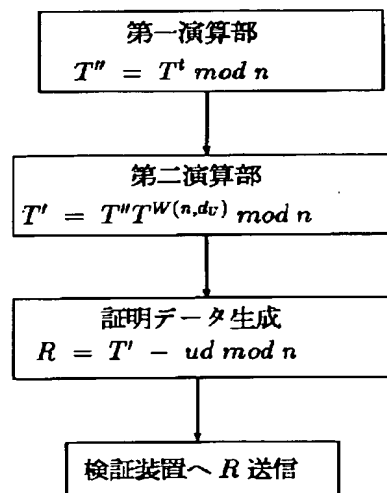
実施例4の証明装置の構成

【図16】



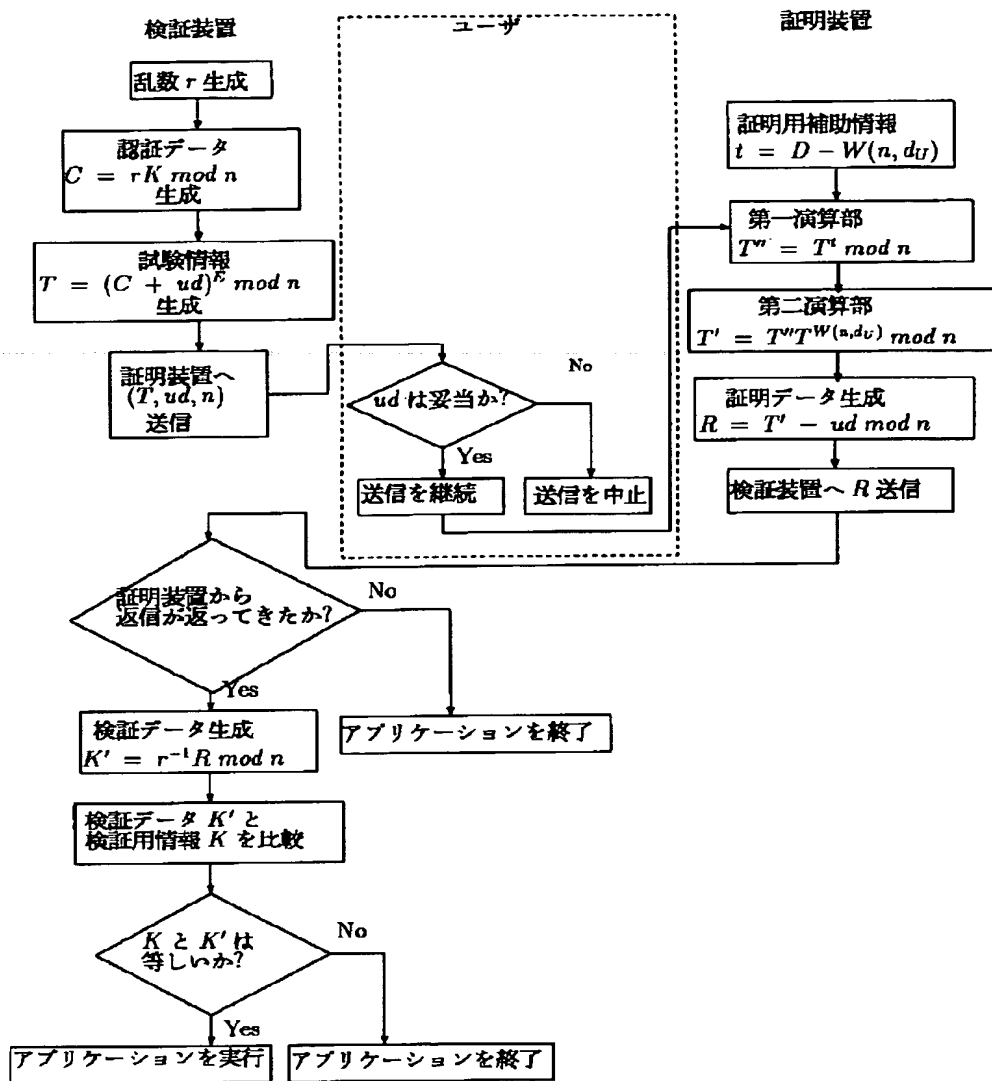
実施例4における検証装置での処理

【図17】



実施例4における証明装置での処理

【図15】



実施例4の処理の流れ

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**